



Trabajo con AWS CloudTrail



INTRODUCCIÓN

AWS CloudTrail permite realizar auditorías, supervisar la seguridad y solucionar problemas operativos mediante el seguimiento de la actividad del usuario y el uso de la API . CloudTrail registra, supervisa de forma continua y conserva la actividad de la cuenta relacionada con las acciones en toda su infraestructura de AWS, lo que le permite controlar el almacenamiento, el análisis y las acciones de reparación.

OBJETIVOS

- Crear y Configurar un rastro de CloudTrail.
- Analice los registros de CloudTrail mediante varios métodos para descubrir información relevante.
- Importar datos de registro de CloudTrail a Athena.
- Ejecutar consultas en Athena para filtrar las entradas de registro de CloudTrail.
- Resolver problemas de seguridad dentro de la cuenta de AWS y en una instancia EC2 de Linux.



TAREA 1

En esta se procede a modificar un grupo de seguridad y observar el sitio web.

- o EnDesde el menú Servicios, seleccione Computación y luego el servicio EC2.
- o Seleccione Instancias y luego localice y seleccione la instancia Café Web Server (WebSecurityGroup).

Instancias (1/2)

Información

Última actualización
Hace 1 minute

Conectar

Estado de la instancia

Acciones

Lanzar instancias

Buscar Instancia por atributo o etiqueta (case-sensitive)

Todos los estados

Estado de la instancia = running

Quitar los filtros

1

<div></div>	Name <div></div>	ID de la instancia	Estado de la i... <div></div>	Tipo de inst... <div></div>	Comprobación de	Estado de la ali	Zona c
<div></div>	HackerInstance	i-0352b03fbd765ca96	<div></div> En ejecución <div></div> <div></div>	t3.micro	<div></div> Inicializando	<div>Ver alarmas</div> <div>+</div>	us-wes
<div></div>	Cafe Web Server	i-00b367c31ab3b37de	<div></div> En ejecución <div></div> <div></div>	t3.micro	<div></div> Inicializando	<div>Ver alarmas</div> <div>+</div>	us-wes

- o En la pestaña Seguridad, elija el grupo de seguridad sg-XXXXXXXXXX.

i-00b367c31ab3b37de (Cafe Web Server)

Detalles

Estado y alarmas

Monitoreo

Seguridad

Redes

Almacenamiento

Etiquetas

▼ Detalles de seguridad

Rol de IAM

c126711a3165897l7843718t1w749347623819-CafelamRole-aYkJa8cjQJWC

ID del propietario

749347623819

Hora de lanzamiento

Thu Oct 10 2024 18:06:59 GMT-0500 (hora estándar de Perú)

Grupos de seguridad

sg-06cf6b9923756579f (WebSecurityGroup)



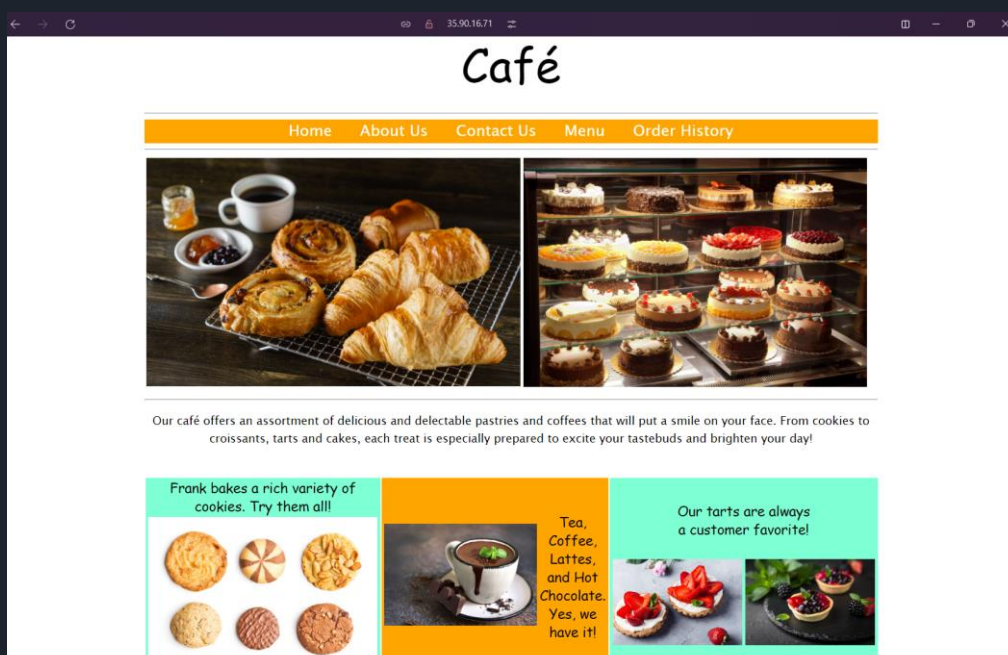
- o En la pestaña Reglas de entrada, observe que solo se ha definido una regla de entrada, que es para el acceso HTTP a través del puerto TCP 80.

Reglas de entrada (1)								Administrar etiquetas	Editar reglas de entrada
<input type="text" value="Buscar"/>							< 1 >		
<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo				
<input type="checkbox"/>	-	sgr-0b6902ab3aba770...	IPv4	HTTP	TCP				

- o Seleccione Editar reglas de entrada y luego seleccione Agregar regla y configure la regla de la siguiente manera:

Reglas de entrada Información						
ID de la regla del grupo de seguridad	Tipo Información	Protocolo Información	Intervalo de puertos Información	Origen Información	Descripción: opcional Información	
sgr-0b6902ab3aba7709b	HTTP	TCP	80	Pers...	<input type="text" value="0.0.0.0"/>	<input type="text" value="Eliminar"/>
-	SSH	TCP	22	Mi IP	<input type="text" value="38.250.153.38/32"/>	<input type="text" value="Eliminar"/>
<input type="button" value="Agregar regla"/>						

- o En la parte inferior de la página, seleccione Guardar reglas.
- o Consulte el sitio web del Café:





TAREA 2

En esta tarea, creas un rastro de CloudTrail en tu cuenta de AWS. También notas que, poco después de crear el rastro, el sitio web de Café es hackeado.

- En la consola de administración de AWS, en el menú Servicios, seleccione Administración y gobernanza y, luego, CloudTrail. Ignore el mensaje de acceso denegado a AWSOrganizations que aparece en la parte superior de la consola.
- En el panel de navegación de la izquierda, seleccione Senderos.
- Seleccione Crear ruta.
- Configure la ruta de la siguiente manera:



Detalles generales

Un registro de seguimiento creado en la consola es un registro de seguimiento de varias regiones. [Más información](#)

Nombre del registro de seguimiento

Escriba un nombre de visualización para el registro de seguimiento.

monitor

De 3 a 128 caracteres. Solo se permiten letras, números, puntos, guiones bajos y guiones.

☐ Habilitar para todas las cuentas de mi organización

Para revisar las cuentas de su organización, abra AWS Organizations. [Ver todas las cuentas](#)

Ubicación de almacenamiento

☒ Crear un bucket de S3 nuevo

Cree un bucket para almacenar los registros del registro de seguimiento.

☐ Usar un bucket de S3 existente

Elija un bucket existente para almacenar los registros de este registro de seguimiento.

Bucket y carpeta del registro de seguimiento

Escriba un nuevo nombre de bucket de S3 y una carpeta (prefijo) para almacenar los registros. Los nombres de bucket deben ser únicos a nivel global.

monitoring1234

Los registros se almacenarán en monitoring1234/AWSLogs/749347623819

Cifrado SSE-KMS para archivo de registro

[Información](#)

☒ Habilitado

Clave de AWS KMS administrada por el cliente

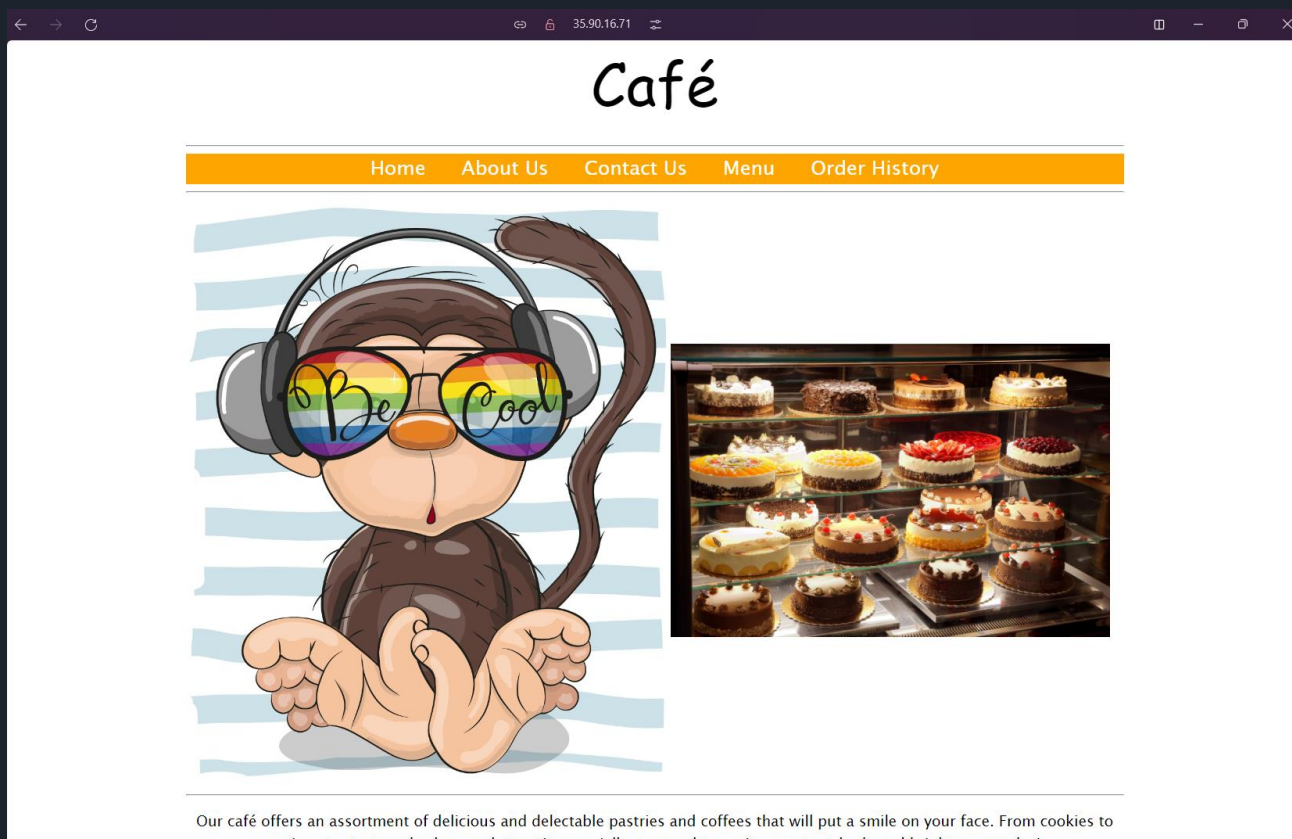
☒ Nuevo

☐ Existente

Alias de AWS KMS

jg-KMC

- Elija Siguiente.
- En la página Elegir eventos de registro, seleccione Siguiente
- En la página Revisar y crear, seleccione Crear ruta
- Verifica que veas tu sendero en la página Senderos.
- Regrese a la pestaña del navegador donde tiene abierto el sitio web de Café y actualice la página.



- o En la consola de administración de AWS, navegue hasta el servicio EC2 y observe los detalles de la instancia del servidor web Café.
- o En la pestaña Seguridad, elija nuevamente el grupo de seguridad sg-xxxxxxx y luego elija la pestaña Reglas de entrada.

i-00b367c31ab3b37de (Cafe Web Server)

CatelamRole-aYkJa8cjQJWC

Grupos de seguridad

sg-06cf6b9923756579f (WebSecurityGroup)

▼ Reglas de entrada

Nombre	ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Origen
-	sgr-0b6902ab3aba7709b	80	TCP	0.0.0.0/0
-	sgr-05b11b4a53cdeee5d	22	TCP	0.0.0.0/0
-	sgr-0a1915b15640cfdda	22	TCP	38.250.153.38/32



```
ec2-user@web-server:~/ctraillogs x + v
[ec2-user@web-server ~]$ cd ctraillogs
[ec2-user@web-server ctraillogs]$ |
```

- Ejecute el siguiente comando para enumerar los depósitos y recuperar el nombre del depósito:

```
ec2-user@web-server:~/ctraillogs x + v
[ec2-user@web-server ctraillogs]$ aws s3 ls
2024-10-10 23:08:41 cafeimagefiles41364
2024-10-10 23:23:15 monitoring1889
[ec2-user@web-server ctraillogs]$ |
```

- En el siguiente comando, reemplace <monitoring#### > con el nombre del depósito real que comienza con monitoring (el nombre del depósito es parte del resultado del ls comando que ejecutó). Ejecute el comando modificado para descargar los registros de CloudTrail:

```
ec2-user@web-server:~/ctraillogs x + v
[ec2-user@web-server ctraillogs]$ aws s3 cp s3://monitoring1889/ . --recursive
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-east-1/2024/10/10/749347623819_CloudTrail_us-east-1_20241010T2330Z_ND5pAoXjbdHz9a5z.json.gz to AWSLogs/749347623819/CloudTrail/us-east-1/2024/10/10/749347623819_CloudTrail_us-east-1_20241010T2330Z_ND5pAoXjbdHz9a5z.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2335Z_ayQRKabZ5Q40075g.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2335Z_ayQRKabZ5Q40075g.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-east-1/2024/10/10/749347623819_CloudTrail_us-east-1_20241010T2330Z_4TyD4HZvYMLl8j8R.json.gz to AWSLogs/749347623819/CloudTrail/us-east-1/2024/10/10/749347623819_CloudTrail_us-east-1_20241010T2330Z_4TyD4HZvYMLl8j8R.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2340Z_yTeR5YrB2QvRvUsh.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2340Z_yTeR5YrB2QvRvUsh.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2330Z_qw4a61f44YqQZchh.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2330Z_qw4a61f44YqQZchh.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2340Z_yz3XeNT6xbYiW0El.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2340Z_yz3XeNT6xbYiW0El.json.gz
download: s3://monitoring1889/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2335Z_tnUsZARlmSNpZKTt.json.gz to AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10/749347623819_CloudTrail_us-west-2_20241010T2335Z_tnUsZARlmSNpZKTt.json.gz
[ec2-user@web-server ctraillogs]$ |
```

- Utilice los comandos `cd` y `ls` repetidamente (o ingrese `cd` luego presione Tab varias veces) según sea necesario para cambiar el directorio al subdirectorio donde se descargaron los registros. Cuando ejecute `ls`, se deben mostrar todos los archivos de registro descargados. Se ubicarán en un



subdirectorio AWSLogs/ < account-num > /CloudTrail/ < Region > / < yyyy > / < mm > / < dd >.

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server ctraillogs]$ ls
AWSLogs
[ec2-user@web-server ctraillogs]$ cd AWSLogs/
[ec2-user@web-server AWSLogs]$ ls
749347623819
[ec2-user@web-server AWSLogs]$ cd 749347623819/
[ec2-user@web-server 749347623819]$ ls
CloudTrail
[ec2-user@web-server 749347623819]$ cd CloudTrail/
[ec2-user@web-server CloudTrail]$ ls
us-east-1 us-west-2
[ec2-user@web-server CloudTrail]$ cd us-west-2/
[ec2-user@web-server us-west-2]$ ls
2024
[ec2-user@web-server us-west-2]$ cd 2024/
[ec2-user@web-server 2024]$ ls
10
[ec2-user@web-server 2024]$ cd 10/
[ec2-user@web-server 10]$ ls
10
[ec2-user@web-server 10]$ cd 10/
[ec2-user@web-server 10]$ ls
749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json.gz
749347623819_CloudTrail_us-west-2_20241010T2330Z_qw4a61f44YqQZchh.json.gz
749347623819_CloudTrail_us-west-2_20241010T2335Z_ayQRKabZ5Q40075g.json.gz
749347623819_CloudTrail_us-west-2_20241010T2335Z_tnUsZARlmSNpZKTt.json.gz
749347623819_CloudTrail_us-west-2_20241010T2340Z_yTeR5YrB2QvRvUsh.json.gz
749347623819_CloudTrail_us-west-2_20241010T2340Z_yz3XeNT6xbYiW0El.json.gz
[ec2-user@web-server 10]$ |
```

- Ejecute el siguiente comando para extraer los registros:
- Ejecute ls nuevamente. Observe que todos los archivos ya están extraídos.

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ gunzip *.gz
[ec2-user@web-server 10]$ ls
749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json
749347623819_CloudTrail_us-west-2_20241010T2330Z_qw4a61f44YqQZchh.json
749347623819_CloudTrail_us-west-2_20241010T2335Z_ayQRKabZ5Q40075g.json
749347623819_CloudTrail_us-west-2_20241010T2335Z_tnUsZARlmSNpZKTt.json
749347623819_CloudTrail_us-west-2_20241010T2340Z_yTeR5YrB2QvRvUsh.json
749347623819_CloudTrail_us-west-2_20241010T2340Z_yz3XeNT6xbYiW0El.json
[ec2-user@web-server 10]$ |
```

- Para analizar la estructura de los registros, haga lo siguiente:



```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ cat 749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json | python -m json.tool
{
  "Records": [
    {
      "awsRegion": "us-west-2",
      "eventCategory": "Management",
      "eventID": "69a86f3c-01e9-4b99-849d-4cb323d2dba8",
      "eventName": "DescribeInstances",
      "eventSource": "ec2.amazonaws.com",
      "eventTime": "2024-10-10T23:23:30Z",
      "eventType": "AwsApiCall",
      "eventVersion": "1.10",
      "managementEvent": true,
      "readOnly": true,
      "recipientAccountId": "749347623819",
      "requestID": "09405b6f-3e0a-4faf-9884-b22184e9b0f2",
      "requestParameters": {
        "filterSet": {},
        "instancesSet": {}
      },
      "responseElements": null,
      "sourceIPAddress": "35.90.16.71",
      "tlsDetails": {
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-west-2.amazonaws.com",
        "tlsVersion": "TLSv1.2"
      },
      "userAgent": "aws-cli/1.18.147 Python/2.7.18 Linux/4.14.352-268.568.amzn2.x86_64 botocore/1.18.6",
      "userIdentity": {
```

- o Ejecute el siguiente comando para establecer la dirección WebServerIP como una variable que puede usar en comandos futuros (reemplace < WebServerIP > con la dirección IP real que se muestra a la izquierda de estas instrucciones):

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ ip=35.90.16.71
[ec2-user@web-server 10]$ |
```

- o Ejecute el siguiente comando:

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ for i in $(ls); do echo $i && cat $i | python -m json.tool | grep sourceIPAddress ; done
749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "35.90.16.71",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
"sourceIPAddress": "38.250.153.38",
```



- Ejecute un comando con una estructura similar pero donde el comando devuelva el eventName de cada evento capturado:

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10
[ec2-user@web-server 10]$ for i in $(ls); do echo $i && cat $i | python -m json.tool | grep eventName ; done
749347623819_CloudTrail_us-west-2_20241010T2330Z_RVJXyp9EXkU6Fa08.json
  "eventName": "DescribeInstances",
  "eventName": "DescribeSecurityGroups",
  "eventName": "DescribeSecurityGroups",
  "eventName": "CreateSecurityGroup",
  "eventName": "GetParametersByPath",
  "eventName": "GetParametersByPath",
  "eventName": "CreateSecurityGroup",
  "eventName": "CreateSecurityGroup",
  "eventName": "CreateSecurityGroup",
  "eventName": "AuthorizeSecurityGroupIngress",
  "eventName": "GetParametersByPath",
  "eventName": "GetParametersByPath",
  "eventName": "GetParametersByPath",
  "eventName": "DescribeVolumes",
  "eventName": "DescribeKeyPairs",
  "eventName": "DescribeVolumeStatus",
  "eventName": "DescribeAccountAttributes",
  "eventName": "DescribeInstanceTypes",
  "eventName": "ListNotificationHubs",
  "eventName": "DescribeSecurityGroups",
749347623819_CloudTrail_us-west-2_20241010T2330Z_qw4a61f44YqQZchh.json
  "eventName": "DescribeInstances",
  "eventName": "DescribeInstances",
  "eventName": "DescribeSecurityGroups",
  "eventName": "DescribeInstances",
  "eventName": "DescribeSecurityGroups",
  "eventName": "DescribeSecurityGroups",
  "eventName": "DescribeSecurityGroups",
```

- Abra la página de referencia de AWS CLI para CloudTrail.
- Elija el comando lookup-events para ver detalles sobre el comando.

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10
[ec2-user@web-server 10]$ aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=Console
Login
{
  "Events": []
}
[ec2-user@web-server 10]$
```

- Ejecute el siguiente comando para encontrar las acciones que se realizaron en los grupos de seguridad en la cuenta de AWS:



```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ aws cloudtrail lookup-events --lookup-attributes AttributeKey=ResourceType,AttributeValue=AWS:
:EC2::SecurityGroup --output text
EVENTS AKIA246EZKOF6S6XFZOL {"eventVersion":"1.10","userIdentity":{"type":"IAMUser","principalId":"AIDA246EZKOF503LJ
TDC3","arn":"arn:aws:iam::749347623819:user/chaos","accountId":"749347623819","accessKeyId":"AKIA246EZKOF6S6XFZOL","user
Name":"chaos"},"eventTime":"2024-10-10T23:24:40Z","eventSource":"ec2.amazonaws.com","eventName":"AuthorizeSecurityGroupI
ngress","awsRegion":"us-west-2","sourceIPAddress":"35.90.16.71","userAgent":"aws-cli/1.18.147 Python/2.7.18 Linux/4.14.3
52-268.568.amzn2.x86_64 boto3/1.18.6","requestParameters":{"groupId":"sg-06cf6b9923756579f","ipPermissions":{"items":
[{"ipProtocol":"tcp","fromPort":22,"toPort":22,"groups":{"ipRanges":{"items":[{"cidrIp":"0.0.0.0/0"}]},"ipv6Ranges":{"
","prefixListIds":{"}}}}},"responseElements":{"requestId":"13aa614c-985a-45d4-98ab-0c02f4fc4915","return":true,"securityG
roupRuleSet":{"items":[{"groupOwnerId":"749347623819","groupId":"sg-06cf6b9923756579f","securityGroupRuleId":"sgr-05b11b
4a53cdeee5d","isEgress":false,"ipProtocol":"tcp","fromPort":22,"toPort":22,"cidrIpv4":"0.0.0.0/0"}]},"requestID":"13aa6
14c-985a-45d4-98ab-0c02f4fc4915","eventID":"c3e9af28-ab5d-405f-9d60-131267004ab7","readOnly":false,"eventType":"AwsApiCa
ll","managementEvent":true,"recipientAccountId":"749347623819","eventCategory":"Management","tlsDetails":{"tlsVersion":"
TLSv1.2","cipherSuite":"ECDHE-RSA-AES128-GCM-SHA256","clientProvidedHostHeader":"ec2.us-west-2.amazonaws.com"}} c3e9af28
-ab5d-405f-9d60-131267004ab7 AuthorizeSecurityGroupIngress ec2.amazonaws.com 1728602680.0 false chaos
RESOURCES sg-06cf6b9923756579f AWS::EC2::SecurityGroup
EVENTS AKIA246EZKOF2KK6LZ47 {"eventVersion":"1.10","userIdentity":{"type":"IAMUser","principalId":"AIDA246EZKOF2S7ZL
PUNQ","arn":"arn:aws:iam::749347623819:user/awstudent","accountId":"749347623819","accessKeyId":"AKIA246EZKOF2KK6LZ47",
"userName":"awstudent"},"eventTime":"2024-10-10T23:24:38Z","eventSource":"ec2.amazonaws.com","eventName":"CreateSecurit
yGroup","awsRegion":"us-west-2","sourceIPAddress":"35.90.16.71","userAgent":"aws-cli/1.18.147 Python/2.7.18 Linux/4.14.3
52-268.568.amzn2.x86_64 boto3/1.18.6","requestParameters":{"groupName":"securitygroup25","groupDescription":"security
group25"},"responseElements":{"requestId":"bcab7b0e-0c03-4fa2-9715-a0ce6cc1ee52","return":true,"groupId":"sg-00bd07c10d
aab3bf7","requestID":"bcab7b0e-0c03-4fa2-9715-a0ce6cc1ee52","eventID":"39360cf8-4e97-4365-9a70-745078d27111","readOnly":
false,"eventType":"AwsApiCall","managementEvent":true,"recipientAccountId":"749347623819","eventCategory":"Management",
"tlsDetails":{"tlsVersion":"TLSv1.2","cipherSuite":"ECDHE-RSA-AES128-GCM-SHA256","clientProvidedHostHeader":"ec2.us-west
-2.amazonaws.com"}} 39360cf8-4e97-4365-9a70-745078d27111 CreateSecurityGroup ec2.amazonaws.com 17286026
78.0 false awstudent
RESOURCES securitygroup25 AWS::EC2::SecurityGroup
RESOURCES sg-00bd07c10daab3bf7 AWS::EC2::SecurityGroup
EVENTS AKIA246EZKOF2KK6LZ47 {"eventVersion":"1.10","userIdentity":{"type":"IAMUser","principalId":"AIDA246EZKOF2S7ZL
```

- o Ejecute los siguientes comandos para encontrar el ID del grupo de seguridad que utiliza la instancia del servidor web Café y luego repita el resultado en la terminal:

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ region=$(curl http://169.254.169.254/latest/dynamic/instance-identity/document|grep region | c
ut -d '"' -f4)
ag:Name,Values='Cafe Web Server' % Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 474 100 474 0 0 175k 0 --:--:-- --:--:-- --:--:-- 231k
[ec2-user@web-server 10]$ sgId=$(aws ec2 describe-instances --filters "Name=tag:Name,Values='Cafe Web Server'" --query '
Reservations[*].Instances[*].SecurityGroups[*].[GroupId]' --region $region --output text)
[ec2-user@web-server 10]$ echo $sgId
sg-06cf6b9923756579f
[ec2-user@web-server 10]$ |
```

- o Ahora use el ID del grupo de seguridad que devolvió el comando anterior para filtrar aún más los resultados del comando CloudTrail de AWS CLI:

```
ec2-user@web-server:~/ctraillogs/AWSLogs/749347623819/CloudTrail/us-west-2/2024/10/10 x + v
[ec2-user@web-server 10]$ aws cloudtrail lookup-events --lookup-attributes AttributeKey=ResourceType,AttributeValue=AWS:
:EC2::SecurityGroup --region $region --output text | grep $sgId
EVENTS AKIA246EZKOF6S6XFZOL {"eventVersion":"1.10","userIdentity":{"type":"IAMUser","principalId":"AIDA246EZKOF503LJ
TDC3","arn":"arn:aws:iam::749347623819:user/chaos","accountId":"749347623819","accessKeyId":"AKIA246EZKOF6S6XFZOL","user
Name":"chaos"},"eventTime":"2024-10-10T23:24:40Z","eventSource":"ec2.amazonaws.com","eventName":"AuthorizeSecurityGroupI
ngress","awsRegion":"us-west-2","sourceIPAddress":"35.90.16.71","userAgent":"aws-cli/1.18.147 Python/2.7.18 Linux/4.14.3
52-268.568.amzn2.x86_64 boto3/1.18.6","requestParameters":{"groupId":"sg-06cf6b9923756579f","ipPermissions":{"items":
[{"ipProtocol":"tcp","fromPort":22,"toPort":22,"groups":{"ipRanges":{"items":[{"cidrIp":"0.0.0.0/0"}]},"ipv6Ranges":{"
","prefixListIds":{"}}}}},"responseElements":{"requestId":"13aa614c-985a-45d4-98ab-0c02f4fc4915","return":true,"securityG
roupRuleSet":{"items":[{"groupOwnerId":"749347623819","groupId":"sg-06cf6b9923756579f","securityGroupRuleId":"sgr-05b11b
4a53cdeee5d","isEgress":false,"ipProtocol":"tcp","fromPort":22,"toPort":22,"cidrIpv4":"0.0.0.0/0"}]},"requestID":"13aa6
14c-985a-45d4-98ab-0c02f4fc4915","eventID":"c3e9af28-ab5d-405f-9d60-131267004ab7","readOnly":false,"eventType":"AwsApiCa
ll","managementEvent":true,"recipientAccountId":"749347623819","eventCategory":"Management","tlsDetails":{"tlsVersion":"
TLSv1.2","cipherSuite":"ECDHE-RSA-AES128-GCM-SHA256","clientProvidedHostHeader":"ec2.us-west-2.amazonaws.com"}} c3e9af28
-ab5d-405f-9d60-131267004ab7 AuthorizeSecurityGroupIngress ec2.amazonaws.com 1728602680.0 false chaos
RESOURCES sg-06cf6b9923756579f AWS::EC2::SecurityGroup
```



TAREA 4

En esta tarea, utilizará Athena para analizar sus registros de CloudTrail.

- Desde el menú Servicios de la consola de administración de AWS, elija CloudTrail para abrir la consola de CloudTrail.
- En el panel de navegación, seleccione Historial de eventos.
- Desde la página Historial de eventos, haga clic en Crear tabla de Athena.
- Tómese un momento para analizar cómo se forma la declaración CREATE TABLE de Athena.

Historial de eventos (50+) Información							Descargar eventos ▼	Crear tabla de Athena
El historial de eventos muestra los últimos 90 días de eventos de administración.								
Atributos de búsqueda								
Solo lectura ▼		Q false X		Filtrar por fecha y hora		< 1 2 ... > ⚙		
<input type="checkbox"/>	Nombre del evento	Hora del evento	Nombre de usuario	Origen del evento	Tipo de recurso			
<input type="checkbox"/>	UpdateInstanceInfor...	octubre 10, 2024, 18:53:25 (UT...	i-00b367c31ab3b...	ssm.amazonaws.com	-			
<input type="checkbox"/>	UpdateInstanceInfor...	octubre 10, 2024, 18:48:25 (UT...	i-00b367c31ab3b...	ssm.amazonaws.com	-			
<input type="checkbox"/>	UpdateInstanceInfor...	octubre 10, 2024, 18:43:25 (UT...	i-00b367c31ab3b...	ssm.amazonaws.com	-			
<input type="checkbox"/>	UpdateInstanceInfor...	octubre 10, 2024, 18:38:25 (UT...	i-00b367c31ab3b...	ssm.amazonaws.com	-			
<input type="checkbox"/>	UpdateInstanceInfor...	octubre 10, 2024, 18:37:13 (UT...	i-00b367c31ab3b...	ssm.amazonaws.com	-			

- Una vez que haya terminado de analizar los detalles de CREAR TABLA, seleccione Crear tabla.



Crear una tabla en Amazon Athena

Puede utilizar Amazon Athena para analizar eventos almacenados en el bucket de Amazon S3 de un registro de seguimiento. Athena es un servicio de consultas interactivo que le ayuda a analizar datos en buckets de S3 mediante SQL estándar. Athena cobra por realizar consultas.[Más información](#)

Ubicación de almacenamiento

monitoring1889

Elija un bucket de S3 que contenga archivos de registro de CloudTrail

Nombre de tabla de Athena

cloudtrail_logs_monitoring1889

Este nombre se genera automáticamente y puede cambiarlo en Amazon Athena.

Consulta de la tabla de Athena

Copiar

```
1 CREATE EXTERNAL TABLE cloudtrail_logs_monitoring1889 (  
2   eventVersion STRING,  
3   userIdentity STRUCT<  
4     type: STRING,  
5     principalId: STRING,  
6     arn: STRING,  
7     accountId: STRING,  
8     invokedBy: STRING,  
9     accessKeyId: STRING,  
10    userName: STRING,  
11    sessionContext: STRUCT<  
12      attributes: STRUCT<  
13        mfaAuthenticated: STRING,  
14        creationDate: STRING>,  
15    sessionIssuer: STRUCT<
```

Cancelar Crear una tabla

- o Desde el menú Servicios, seleccione Análisis y luego el servicio Athena.
- o Si aún no ve el Editor de consultas de Athena, seleccione Explorar editor de consultas y debería aparecer.
- o En el panel izquierdo del Editor de consultas de Athena, debería ver la tabla cloudtrail_logs_monitoring####.

Tablas (1)		< 1 >
cloudtrail_logs_monitoring1889		
eventversion	string	
useridentity		
struct<type:string,principalId:string,arn:string,accountId:string,invokedBy:string,accessKeyId:string,userName:string,sessionContext:struct<attributes:struct<mfaAuthenticated:string,creationDate:string>,sessionIssuer:struct<type:string,principalId:string,arn:string,accountId:string,userName:string>,ec2RoleDelivery:string,webIdFederationData:map<string,string>>>		
eventtime	string	
eventsources	string	
eventname	string	
awsregion	string	
sourceipaddress	string	
useragent	string	



- Comience configurando una ubicación para los resultados de la consulta y luego ejecute una consulta simple para tener una idea de los datos que están disponibles en los registros.

Ubicación y codificación de los resultados de la consulta

Location of query result - *optional*
Enter an S3 prefix in the current region where the query result will be saved as an object.

You can create and manage lifecycle rules for this bucket
Use Amazon S3 lifecycle rules to store your query results and metadata cost effectively or to delete them after a period of time.
[Learn more](#)

Expected bucket owner - *optional*
Specify the AWS account ID that you expect to be the owner of your query results output location bucket.

☐ Assign bucket owner full control over query results
Enabling this option grants the owner of the S3 query results bucket full control over the query results. This means that if your query result location is owned by another account, you grant full control over your query results to the other account.

☐ Encrypt query results

Resultados de la consulta		Estado de la consulta	
✓ Completado		Tiempo en cola: 59 ms	Tiempo de ejecución: 673 ms
		Datos analizados: 8.29 KB	
Resultados (5)		<input type="button" value="Copiar"/>	<input type="button" value="Descargar resultados"/>
<input type="text" value="Filas de búsqueda"/>			
#	eventversion	useridentity	
1	1.09	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com}	
2	1.10	{type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com}	
3	1.09	{type=AssumedRole, principalid=AROIA246EZKOFYSTCEAKRH:user3386630=Joseph_Julios, a}	
4	1.09	{type=AssumedRole, principalid=AROIA246EZKOFYSTCEAKRH:user3386630=Joseph_Julios, a}	
5	1.09	{type=AssumedRole, principalid=AROIA246EZKOFYSTCEAKRH:user3386630=Joseph_Julios, a}	

- Ejecute una nueva consulta que seleccione únicamente las columnas mencionadas anteriormente. Esta vez, limite los resultados a 30 filas:

```
1 SELECT useridentity.userName, eventtime, eventsources, eventname, requestparameters
2 FROM cloudtrail_logs_monitoring1889
3 LIMIT 30
```




Resultados de la consulta		Estado de la consulta		
✔ Completado		Tiempo en cola: 100 ms	Tiempo de ejecución: 661 ms	Datos analizados: 16.83 KB
Resultados (30)				
			Copiar	Descargar resultados
🔍 Filas de búsqueda			< 1 > ⚙	
# ▼	userName ▼	eventtime ▼	eventsources ▼	eventname
1		2024-10-11T00:04:14Z	organizations.amazonaws.com	DescribeOrganization
2		2024-10-11T00:05:13Z	iam.amazonaws.com	ListRoles
3		2024-10-11T00:05:09Z	kms.amazonaws.com	GenerateDataKey
4		2024-10-11T00:05:09Z	s3.amazonaws.com	GetBucketAcl
5		2024-10-11T00:05:13Z	kms.amazonaws.com	DescribeKey
6		2024-10-11T00:05:13Z	athena.amazonaws.com	ListWorkGroups
7		2024-10-11T00:05:16Z	athena.amazonaws.com	ListDataCatalogs
8		2024-10-11T00:05:13Z	athena.amazonaws.com	ListWorkGroups
9		2024-10-11T00:05:16Z	athena.amazonaws.com	ListQueryExecutions



Desafío: Identifica al Hacker

En esta sección de la actividad, intenta descubrir la entrada del registro que incluye la información esencial sobre quién hackeó el sitio web. No se proporcionan pasos específicos. En su lugar, debes experimentar ejecutando distintas consultas hasta que encuentres la información que estás buscando.

✓ Consulta 1 ⋮

1 SELECT DISTINCT useridentity.userName, eventName, eventSource FROM cloudtrail_logs_monitoring1889 WHERE from_iso8601_timestamp(eventtime) > date_add('day', -1, now()) ORDER BY eventSource;

Resultados (93) Copiar Descargar resultados

🔍 Filas de búsqueda < 1 > ⚙️

# ▾	userName ▾	eventName ▾	eventSource ▾
1		ListQueryExecutions	athena.amazonaws.com
2		ListDataCatalogs	athena.amazonaws.com
3		GetQueryRuntimeStatistics	athena.amazonaws.com
4		ListWorkGroups	athena.amazonaws.com
5		GetQueryExecution	athena.amazonaws.com
6		GetQueryResults	athena.amazonaws.com
7		StartQueryExecution	athena.amazonaws.com
8		BatchGetQueryExecution	athena.amazonaws.com
9		GetWorkGroup	athena.amazonaws.com
10		DescribeAutoScalingGroups	autoscaling.amazonaws.com



TAREA 5

En esta última tarea, trabajará para proteger tanto su cuenta de AWS como la instancia del servidor web.

- o En la terminal donde tiene una sesión SSH activa en la instancia del servidor web, ejecute el siguiente comando para averiguar quién ha iniciado sesión recientemente en este sistema operativo (SO):

```
ec2-user@web-server:~$ sudo aureport --auth
Authentication Report
# date time acct host term exe success event
1. 10/10/24 23:24:47 chaos-user ec2-35-88-104-150.us-west-2.compute.amazonaws.com ssh /usr/sbin/sshd yes 137
2. 10/10/24 23:24:47 chaos-user 35.88.104.150 ssh /usr/sbin/sshd yes 140
3. 10/10/24 23:34:36 ec2-user 38.250.153.38 ? /usr/sbin/sshd yes 163
4. 10/10/24 23:34:36 ec2-user 38.250.153.38 ? /usr/sbin/sshd yes 164
5. 10/10/24 23:34:36 ec2-user 38.250.153.38 ssh /usr/sbin/sshd yes 167
6. 10/11/24 00:25:54 ec2-user 38.250.153.38 ? /usr/sbin/sshd yes 241
7. 10/11/24 00:25:54 ec2-user 38.250.153.38 ? /usr/sbin/sshd yes 242
8. 10/11/24 00:25:54 ec2-user 38.250.153.38 ssh /usr/sbin/sshd yes 245
[ec2-user@web-server ~]$
```

- o Ejecute el comando `who` para averiguar quién está conectado actualmente:

```
ec2-user@web-server:~$ who
chaos-user pts/0      2024-10-10 23:24 (ec2-35-88-104-150.us-west-2.compute.amazonaws.com)
ec2-user pts/1      2024-10-11 00:25 (38.250.153.38)
[ec2-user@web-server ~]$
```

- o Ejecute el siguiente comando para intentar eliminar el usuario del sistema operativo `chaos-user`:



```
ec2-user@web-server:~ x + v
[ec2-user@web-server ~]$ sudo userdel -r chaos-user
userdel: user chaos-user is currently used by process 4095
[ec2-user@web-server ~]$
```

- o En el siguiente comando, reemplace ProcNum por el número de proceso devuelto por el último comando. Ejecute el comando modificado para detener el proceso que tiene activa la sesión de inicio de sesión de usuario Chaos:

```
ec2-user@web-server:~ x + v
[ec2-user@web-server ~]$ sudo kill -9 4095
[ec2-user@web-server ~]$ |
```

- o Ejecute el comando who nuevamente para verificar que el usuario del sistema operativo chaos-user ya no esté conectado:

```
ec2-user@web-server:~ x + v
[ec2-user@web-server ~]$ who
ec2-user pts/1      2024-10-11 00:25 (38.250.153.38)
[ec2-user@web-server ~]$ |
```

- o Ejecute el siguiente comando para intentar eliminar el usuario chaos nuevamente:

```
ec2-user@web-server:~ x + v
[ec2-user@web-server ~]$ sudo userdel -r chaos-user
[ec2-user@web-server ~]$ |
```

- o Ejecute el siguiente comando para verificar que no haya otros usuarios sospechosos del sistema operativo que puedan iniciar sesión:



```
ec2-user@web-server:~ X + v
[ec2-user@web-server ~]$ sudo cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
ec2-user:x:1000:1000:EC2 Default User:/home/ec2-user:/bin/bash
[ec2-user@web-server ~]$
```

- o Analizar la configuración de SSH en la instancia.

```
ec2-user@web-server:~ X + v
[ec2-user@web-server ~]$ sudo ls -l /etc/ssh/sshd_config
-rw----- 1 root root 3957 Oct 10 23:08 /etc/ssh/sshd_config
[ec2-user@web-server ~]$
```

- o Ejecute el siguiente comando para editar el archivo de configuración SSH en el editor VI:

```
ec2-user@web-server:~ X + v
[ec2-user@web-server ~]$ sudo vi /etc/ssh/sshd_config
[ec2-user@web-server ~]$ |
```

```
ec2-user@web-server:~ X + v
49 #AuthorizedPrincipalsFile none
50
51
52 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
53 #HostbasedAuthentication no
54 # Change to yes if you don't trust ~/.ssh/known_hosts for
55 # HostbasedAuthentication
56 #IgnoreUserKnownHosts no
57 # Don't read the user's ~/.rhosts and ~/.shosts files
58 #IgnoreRhosts yes
59
60 # To disable tunneled clear text passwords, change to no here!
61 #PasswordAuthentication yes
62 #PermitEmptyPasswords no
63 #PasswordAuthentication no
64
65 # Change to no to disable s/key passwords
66 #ChallengeResponseAuthentication yes
67 ChallengeResponseAuthentication no
68
69 # Kerberos options
70 #KerberosAuthentication no
71 #KerberosOrLocalPasswd yes
72 #KerberosTicketCleanup yes
73 #KerberosGetAFSToken no
74 #KerberosUseKuserok yes
75
76 # GSSAPI options
77 GSSAPIAuthentication yes
```

63,1 43%

- o Ejecute el siguiente comando para reiniciar el servicio SSH para que los cambios surtan efecto:



```
ec2-user@web-server:~  
[ec2-user@web-server ~]$ sudo service sshd restart  
Redirecting to /bin/systemctl restart sshd.service  
[ec2-user@web-server ~]$ |
```

- o Por último, en la consola EC2, regrese a la configuración del grupo de seguridad del servidor web. Eliminar SSH.

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>	
sgr-0b6902ab3aba7709b	HTTP	TCP	80	Pers...	<input type="text" value="0.0.0.0"/>	<input type="button" value="Eliminar"/>
sgr-05b11b4a53cdee5d	SSH	TCP	22	Pers...	<input type="text" value="0.0.0.0"/>	<input type="button" value="Eliminar"/>
sgr-0a1915b15640cfdda	SSH	TCP	22	Pers...	<input type="text" value="38.250.153.38/32"/>	<input type="button" value="Eliminar"/>

- o Guarde el cambio.
- o Ejecute el siguiente comando para navegar al directorio donde se encuentran los archivos de imagen del sitio web y revisar el contenido:

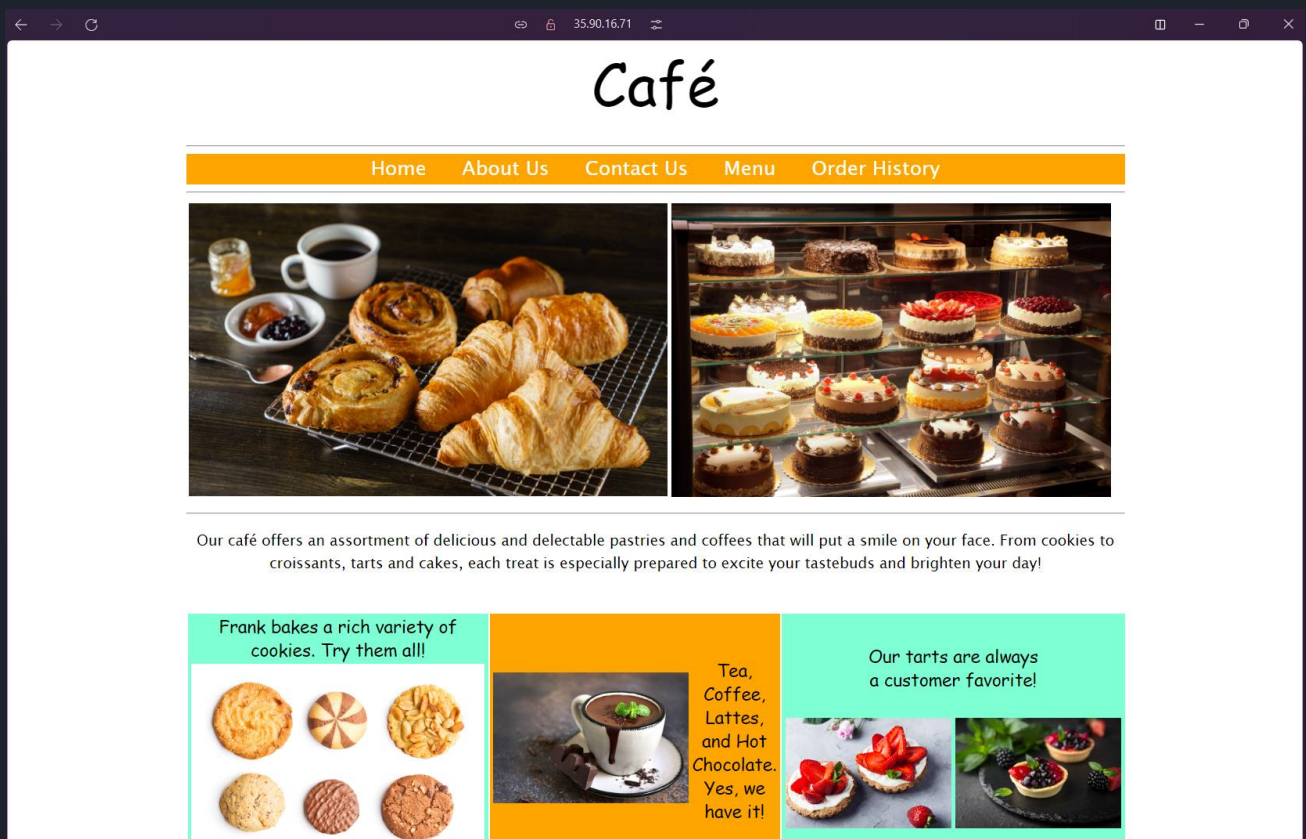
```
ec2-user@web-server:/var/www/html/cafe/images  
[ec2-user@web-server ~]$ cd /var/www/html/cafe/images/  
[ec2-user@web-server images]$ ls -l  
total 5732  
-rwxrwxrwx 1 root root 647353 Apr 2 2019 Cake-Vitrine.jpg  
-rwxrwxrwx 1 root root 480820 Apr 2 2019 Chocolate-Chip-Cookies.jpg  
-rwxrwxrwx 1 root root 17528 Apr 6 2021 Coffee-Shop.png  
-rwxrwxrwx 1 1001 root 486325 Apr 2 2019 Coffee-and-Pastries.backup  
-rw-r--r-- 1 1001 root 260603 Oct 10 23:08 Coffee-and-Pastries.jpg  
-rwxrwxrwx 1 root root 631884 Apr 3 2019 Coffee.jpg  
-rwxrwxrwx 1 root root 429183 Apr 2 2019 Cookies.jpg  
-rwxrwxrwx 1 root root 351781 Apr 2 2019 Croissants.jpg  
-rwxrwxrwx 1 root root 316090 Apr 2 2019 Cup-of-Hot-Chocolate.jpg  
-rwxrwxrwx 1 root root 380753 Apr 2 2019 Donuts.jpg  
-rwxrwxrwx 1 root root 411014 Apr 2 2019 Frank-Martha.jpg  
-rwxrwxrwx 1 root root 319081 Apr 2 2019 Latte.jpg  
-rwxrwxrwx 1 root root 243718 Apr 2 2019 Muffins.jpg  
-rwxrwxrwx 1 root root 290697 Apr 2 2019 Strawberry-Blueberry-Tarts.jpg  
-rwxrwxrwx 1 root root 479213 Apr 2 2019 Strawberry-Tarts.jpg  
-rwxrwxrwx 1 root root 94341 Apr 2 2019 default-image.jpg  
[ec2-user@web-server images]$ |
```



- Ejecute el siguiente comando para restaurar el gráfico original en el sitio web.

```
ec2-user@web-server:var/www/html/cafe/images X + v
[ec2-user@web-server images]$ sudo mv Coffee-and-Pastries.backup Coffee-and-Pastries.jpg
[ec2-user@web-server images]$ |
```

- Para probar la solución, vuelva a cargar el sitio web <http://WebServerIP/cafe> en el navegador.



- En la consola de administración de AWS, elija el menú Servicios y elija IAM.
- Seleccione el enlace Usuarios y seleccione la casilla de verificación junto al usuario Chaos.



Usuarios (1/2) [Información](#)

🔄

Eliminar

Crear usuario

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

< 1 > ⚙️

<input type="checkbox"/>	Nombre de usuario	Ruta	Grupo	Última actividad	MFA	Antigüedad
<input type="checkbox"/>	awsstudent	/	1	✅ hace 43 minutos	-	-
<input checked="" type="checkbox"/>	chaos	/	0	✅ hace 1 hora	-	✅ 1 hora

- Seleccione Eliminar, ingrese el nombre del usuario y seleccione Eliminar.

¿Desea eliminar chaos? ✕

¿Desea eliminar **chaos** de forma permanente? Esto también eliminará todos los datos del usuario, las credenciales de seguridad y las políticas insertadas.

Nombre de usuario	Última actividad
chaos	hace 1 hora

Nota: la actividad reciente suele aparecer en un plazo de 4 horas. Los datos se almacenan durante un máximo de 365 días, dependiendo de cuándo comenzó a admitir esta característica su región. [Más información](#)

Esta acción no se puede deshacer.

Para confirmar la eliminación, introduzca el nombre del usuario en el campo de entrada de texto.

Cancelar

Eliminar usuario